

EXHIBIT D

STATE OF MISSOURI

§

ST. LOUIS COUNTY

§

§

AFFIDAVIT OF HARRY HAURY

Before me, the undersigned notary, on this day personally appeared Harry Haury, whose identity is known to me, who under oath states as follows:

1. I am the acting CEO of Cain & Associates. Among many other roles, I have served the National Security Agency and other agencies as a senior information assurance architect. These broad engagements involving development of critical elements of the U.S. National Infrastructure have extended over a period of over 25 years.
2. On October 4, 2022, the Los Angeles County District Attorney started the seizure of Konnech, Inc.'s electronic servers found at its two corporate locations as well as computers, cell phones and external electronic storage devices found at the home of Konnech's CEO, Eugene Yu. The seizure occurred in Michigan in accordance with a lawful search warrant for the headquarters and a criminal complaint against Mr. Yu.
3. Cain & Associates was tasked with assisting the Los Angeles County District Attorney's Office Bureau of Investigation in the execution of the court-ordered search warrant. I coordinated the physical search for the devices, along with Andrew Stevens, LA County's investigator.
4. Based on my experience, Konnech's system of data protection and access amounted to by far the worst example of complete disregard or negligence regarding the protection of PII and sensitive data I have ever seen. We discovered a breach of U.S. data that is classified as a "total loss of control".
5. During our investigation, Cain & Associates:
 - a. confirmed multiple instances of Konnech hosting, on servers based in China, U.S. citizens' personally identifiable information (PII);
 - b. confirmed thousands of instances of Konnech data, including U.S. citizens' PII, and software being transferred to and from China;
 - c. found evidence in Konnech's private company messages that elections software code was being developed, tested, and maintained in China;

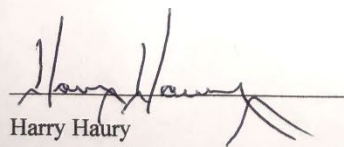
- d. confirmed that Konnech was providing administrative credentials to Chinese developers;
 - e. discovered, more disturbingly, that the Konnech-provided PollChief software used by Los Angeles County (and likely other U.S. jurisdictions) suffered from a security vulnerability that allowed *any* PollChief or Konnech worker to elevate his, her, or own user status to “super user,” giving him or her access to the applications at a privilege above those dictated by security policy which includes broad access to information on all U.S. poll workers in the system;
 - f. obtained evidence that Konnech employees have shared election-related data through, from, and on Chinese servers and applications;
 - g. obtained evidence in downloaded messages that indicated Eugene Yu was involved in developing Chinese government election software; and
 - h. obtained evidence showing Konnech is associated with companies based in mainland China that are subsidized by and have received honors from the Chinese government;
6. I also worked with a confidential informant at the Konnech locations who provided us with usernames and passwords to access various Konnech Internet-connected accounts, such as Jira (used by programmers to report bugs and add software development tasks, or tickets), Konnech’s internal email system, and the China-based collaboration service DingTalk.
 7. However, by about the fourth day following the seizure, someone systematically began shutting off access to these and other accounts, one by one. On information and belief, the restriction of the DA’s access was orchestrated by either Konnech, Inc. or by persons or entities in China with whom Konnech was associated, including any of the many super users on the accounts.
 8. Since becoming aware of Konnech’s breach of PII, we have been in contact with the DCSA and law enforcement in counties that are customers of Konnech, including Allegheny County, PA; Fairfax County, VA; DeKalb County, GA; and Johnson County, KS.
 9. I asked these customers if Konnech had notified them of any data breach, as it is obligated to do, and every person to whom I spoke said that Konnech had given them no

such notification. There is no option but to conclude Konnech has violated its duty to disclose to its customers, the affected counties and municipalities, the PII breach.

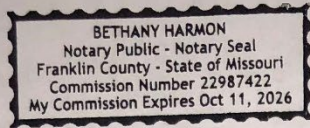
10. We concluded that this incident is a very high risk indicator of an intrusion by a foreign intelligence into the U.S. strategic infrastructure, and as obliged by law, we informed the Defense Counterintelligence and Security Agency (DCSA) and other pertinent law enforcement agencies of this contact.
11. My recommendation is that the seized devices be placed into the temporary custody of an independent forensic examiner to be mirror-imaged. The critical issue is for independent cyber recovery from the equipment to be conducted by one, or more, qualified teams using FBI/DOJ standard recovery techniques either bonded or under affiant pledges.
12. The level of recovery is best if the original equipment is used. The next best would be making bit-by-bit full disk images. The least optimal would be making copies of relevant files. Chain of custody may be maintained by using digital hashes. The parties could then have their own cyber analysis performed using their respective copies. Placing all raw material under a non-disclosure order or appropriate seal would serve to ensure an intact repository to support current and future investigations.
13. On information and belief, and subject to change upon receipt of chain of custody and other information, the list of seized devices includes but is not limited to those in Exhibit F.

I certify under penalty of perjury that the foregoing is true and correct.

Further Affiant Sayeth Not.


Harry Haury

Subscribed to and sworn before me on this ____ day of February, 2023.



Bethany Harmon
Notary Public in and for the state of Missouri